



# The Power-1 Performance Architecture

Delivering Application-layer Security at  
Data Center Performance Levels

# Contents

Introduction .....	3
A delicate balance: Performance and security .....	3
Increased bandwidth requirements .....	4
Increased application-layer threats .....	4
Power-1: High Security for High-Performance Environments .....	5
Open architectures increase in performance value over the solution's life .....	6
Open architectures result in better price/performance for the customer .....	7
The Check Point acceleration technologies .....	7
ClusterXL: Smart load balancing .....	7
SecureXL: Security acceleration .....	8
CoreXL: Multicore acceleration .....	9
Conclusion .....	10

## Introduction

Companies have always faced a tradeoff with network security. Do they lock down the network and face performance issues? Or do they focus on a high level of performance at the expense of preventing possible attacks? Today, these decisions are even harder. Application-layer threats are increasingly the vector of choice of hackers and malware. These attacks—disguised as legitimate traffic—require a deeper level of inspection that needs more processing power. At the same time, companies are beginning to transition to 10G networks. Established as a standard in 2002 10Gigabit Ethernet had a growth rate of almost 60 percent in 2006. Servers, high performance computing clusters, blade servers, storage-area networks and network-attached storage all currently make use of 1G and 10G Ethernet, with 10G growing significantly in 2007 and 2008<sup>1</sup>. 10G Ethernet requires a security solution that can keep up with it in order to maintain a positive return on investment.

Check Point Power-1™ security appliances are designed with these two challenges in mind—raising throughput while simultaneously raising security levels. Rather than make companies choose between performance and security, Power-1 provides the ability to deliver both security and performance in the same platform by providing several layers of patented or patent pending acceleration technologies. These layers work together with advanced technologies, such as multi-core CPUs, to deliver on the promise of application-layer security at high performance levels. This white paper will explain the philosophy behind the Power-1 performance architecture and will explore each of its layers in detail.

### **A delicate balance: Performance and security**

Securing a network is a constant tradeoff. The network is an information access enabler—people want and expect instant access to data, to systems, or to other people in the case of Voice over Internet Protocol (VoIP). On the other hand, security is about limiting the amount of access people have. New regulations and a higher level of security awareness have forced organizations to reexamine their security policies and place more emphasis on security. As an organization becomes increasingly strict about security, the amount of access will decrease.

Complicating matters is the fact that as security controls are increased, the security tools themselves come under a higher workload and, therefore, reduce performance, indirectly affecting access levels. To protect against today's risks of highly advanced attacks and information leakage requires a higher level of inspection as information passes through the perimeter gateway. As more security checks are placed on information, the security tools themselves will face a greater processing load to implement the security policy—effectively slowing down security inspection.

This problem of balancing information access and security is evident in two key areas: Increased bandwidth requirements and rising levels of application-layer threats.

---

<sup>1</sup> Network World, April 9, 2009, “100 Gigabit Ethernet: Bridge to Terabit Ethernet,” Jim Duffy

### Increased bandwidth requirements

Networks are transitioning from 1G to 10G Ethernet. Although this will not immediately translate into increased throughput requirements at the perimeter, security performance requirements will increase on the whole. Besides existing at the perimeter, integrated firewall/VPNs play an important role in separating network segments and segregating important servers in large offices and data centers. Internally, the change to 10G will require firewalls to scale appropriately as well.

Just as large offices deal with securing the backbone or Gigabit Ethernet, small and branch offices will be changing performance paradigms. VoIP and other multimedia applications are growing in use throughout the network, extending to branch and small offices. According to a February 2009 Osterman Research Enterprise VoIP Market Trend study the proportion of VoIP users will continue to grow, from 28% of users in 2008 (up from 20% of users in 2007) to more than 50% in 2010.<sup>2</sup> Because of the low latency/high throughput requirements of multimedia traffic, security performance requirements will increase for branch offices.

### Increased application-layer threats

According to a Verizon Business Report in 2008 hacking led to data breaches by a margin of almost two to one. 39% of the attacks targeting the Application Service Layer led to data compromise.<sup>3</sup> This information quantifies what was already known — attacks are now disguised as legitimate application-layer traffic. The reasoning behind these attacks is that traditional firewall-based security focuses on network-layer access, preventing people from accessing specific IP addresses or networks unless authorized. Modern attacks mean that a supposedly trusted user is disguising the traffic so that it passes the firewall. From a security inspection viewpoint, the answer is to do a deeper level of inspection — similar to intrusion prevention — on the firewall to detect application-layer threats. However, every additional security screening that is done decreases the ability for the firewall to efficiently process the traffic, slowing down its predictable performance.

The traditional method of dealing with increased security performance requirements has been to develop a closed architecture based on application-specific integrated circuits (ASICs) or other specialized hardware. These purpose-built devices are designed to efficiently handle specific tasks much faster than general purpose processors. For some security tasks, such as network address translation (NAT) or basic packet filtering, these closed systems provide a simple way to accelerate security performance.

The problem with closed systems is that application-layer threats are not static — they are dynamic — and closed systems are not designed to respond adequately to these types of threats. After their initial configuration, ASIC-based systems cannot be reprogrammed to address new attacks. To combat these new attacks, closed systems include a general-purpose processor that is field programmable but does not include the acceleration technology found in ASICs. This results in two major issues for closed systems:

---

<sup>2</sup> Osterman Research Enterprise VoIP Market Trends, 2009-2012

<sup>3</sup> Verizon Business Risk Team 2008 Data Breach Investigations Report

1. There are two inspection tracks—fast and slow: For simple tasks, ASICs accelerate the traffic. But for more complex tasks, such as those associated with Web traffic, email, VoIP, or accessing sensitive information, traffic is sent to a secondary processor. This slow track is dependent on bus speeds and on processor power. However, the technologies chosen for these components are of secondary concern to the ASICs and often provide underpowered performance against application-layer threats. Because of this, ASIC-based systems are particularly prone to slow performance as new attacks appear when compared to open systems.
2. Closed systems lose their performance value over time: Because ASICs cannot be programmed in the field to deal with the new threats that appear daily, closed systems start becoming slower the day after the system has been designed. With each additional attack that appears, the closed system will become slower and slower. Over the lifetime of a closed system, it can be expected that the owner will face a choice. Either accept debilitating performance or do not activate any defenses to protect against new attacks.

### **Power-1: High Security for High-Performance Environments**

Power-1 appliances change the security performance equation. Rather than making people choose between having good performance and good security, they provide a framework for people to have both. With top firewall throughputs reaching 25 Gbps at a price of less than \$4.00/Mbps, Power-1 also enables network administrators to gain the security of deep inspection in high performance environments through the IPS Software Blade. For example, a customer who wishes to protect a server farm or DMZ will need protection against HTTP-based worms and for specific server attacks, such as email or FTP. By activating default IPS Policy settings, that customer will still achieve up to 15 Gbps. If that same customer is attempting to protect the internal network from outside threats, he or she will want to activate a more stringent profile—one that controls activities like VoIP, instant messaging, or peer-to-peer file transfers. When activating this strict protection profile, Power-1 gateways will deliver up to 3.4 Gbps of throughput.

To reach these speeds, Power-1 appliances leverage the Check Point Open Performance Architecture, which consists of three patented technologies:

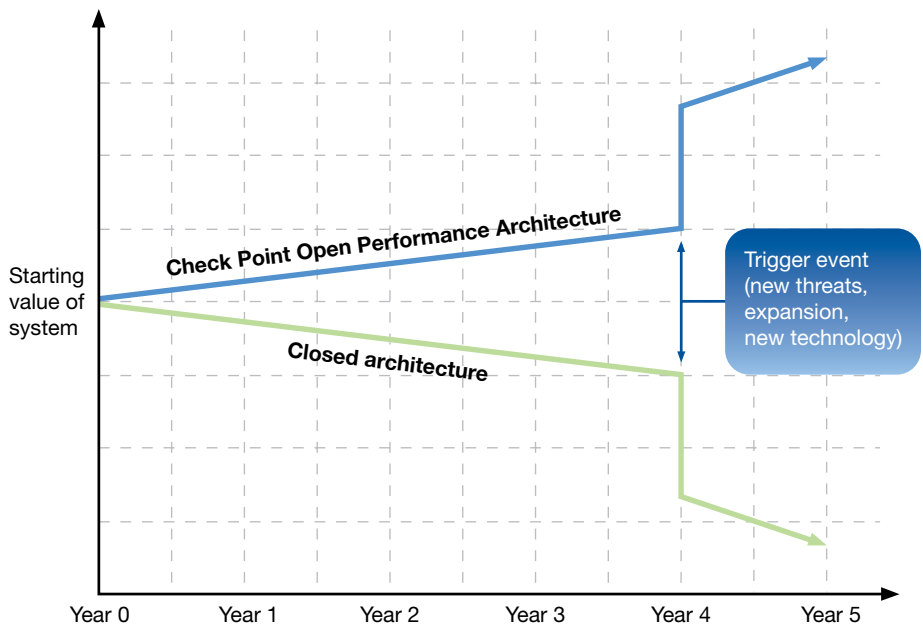
- CoreXL™ Multicore Acceleration—CoreXL multicore acceleration is the first security technology designed to fully leverage multicore processors. It does this by sharing security inspection duties throughout all cores
- SecureXL™ Security Acceleration—SecureXL security acceleration accelerates security inspection by removing the latency introduced as network traffic passes through a security device
- ClusterXL™ Smart Load Balancing—ClusterXL enables near-linear performance increases by clustering together multiple Power-1 appliances

These three technologies work together to fully accelerate security inspection along a unified path that ensures both high performance and high security. In creating these technologies, Check Point followed two key philosophies.

**Open architectures increase in performance value over the solution’s life**

The true value of a security system is not whether it can efficiently deal with the threats you know, but rather the threats that have not appeared yet. A key feature of the Check Point Open Performance Architecture is the ability to adapt to new threats while maintaining a predictable level of performance. It does this by maintaining a unified path of inspection based on the use of commonly available hardware technologies. When a new type of attack appears, Power-1 will not suffer the performance degradation associated with switching from ASIC-based acceleration to general-purpose processors. Rather, the protection will be treated as any existing defense would be processed. This gives customers the knowledge that performance will remain consistent as their security policies adapt.

In comparison, ASIC-based systems start losing value the minute a new attack appears and traffic begins to be transferred to the slower inspection channel. In practice, this results in a steep performance decline when the first deep inspection setting is turned on—anywhere from 95 to 99 percent degradation. It is important to understand that this loss of performance value does not start when the system is purchased. It starts when the system is designed. Toward the end of a particular system’s life cycle, the value is exceptionally low.



The above graph illustrates the concept that two systems—one based on the Check Point Open Performance Architecture and the other a closed architecture—that start with equal performance value, will see a gap quickly appear as new attacks emerge. Complicating matters is the fact that every three to four years, a new paradigm of security, such as the wide adoption of the Web for business or the emergence of Slammer and Conficker worms to welcome the application-layer and network-service attack era, appears that closed systems cannot adapt to. Because of its open nature, the Check Point solution will be able to provide coverage much faster when these large scale security shifts occur.

**Open architectures result in better price/performance for the customer**

Check Point is committed to providing the best security solution available to our customers. Research and development is focused exclusively on technologies that will increase the level of security within customer environments. For hardware platforms, Check Point works closely with microprocessor manufacturers to ensure Check Point solutions take maximum advantage of their research. These partnerships makes the total cost of the combined solution—security plus hardware—much lower. For example, Power-1 will deliver up to 25 Gbps of throughput and cost less than \$4/Mbps. This system will also provide up to 3.4 Gbps of intrusion prevention when a strict security profile is required. The result is a security ecosystem where each partner specializes in its area of expertise, resulting in a cost-efficient solution that is of higher quality at protecting the network than closed systems.

**The Check Point acceleration technologies**

Although there are many factors that go into performance such as hardware improvements and optimized code, the Check Point Open Performance Architecture within Power-1 concentrates on three technologies: ClusterXL, SecureXL, and CoreXL. These three technologies work together to maximize performance across a wide set of open servers and appliances. The next section of the white paper will explain how each technology works.

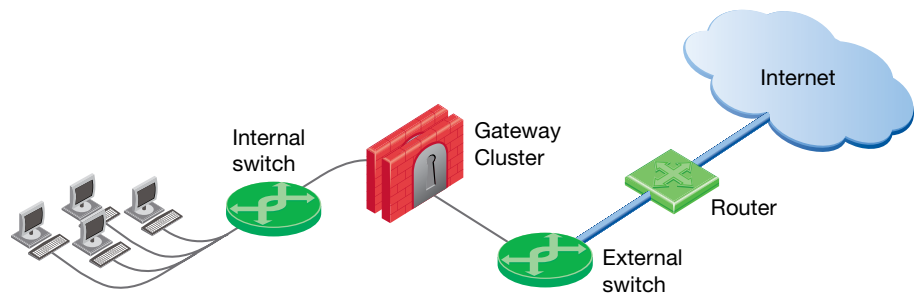
**ClusterXL: Smart load balancing**

ClusterXL provides a method for high traffic volumes to be intelligently spread across multiple gateways. This provides scalability and greatly increases reliability. A gateway cluster can be physically located in a single location or separated and connected via an internal backbone, further increasing the redundancy needed for business continuity.

In operation, each Security Gateway R70 that is a cluster member maintains its own IP address and physical MAC address. To systems that are not part of the cluster, it will appear that all cluster members have a single virtual IP address that represents the cluster. On both the internal and external networks, the gateways will be joined together.

These processes enable information to be shared quickly between cluster members. The communications exchange is used to ensure synchronization of security information and decisions between multiple Security Gateway R70s. This is necessary because network traffic may not exit a network from the same cluster member that was previously used for entry. Sharing firewall, VPN, NAT, and IPS tables is called state synchronization and ensures that if a gateway becomes unavailable, other gateways can allow traffic to continue without interruption. In the event of a failover, the cluster member uses the synchronized state tables to ensure that the security inspection continues as before on the active (non-failed) cluster members.

The actual load sharing decision is made in one of two ways: Unicast or Multicast mode. In Unicast mode, one of the Security Gateway R70s acts as a “pivot,” the coordinator for the cluster. This pivot will receive all incoming traffic and then decides which cluster member will handle the connection or traffic. In Multicast mode, physical network interface cards can be bonded, or joined together, to form a single virtual interface with a single virtual MAC address. This gives the administrator additional flexibility in handling complex deployment scenarios involving multiple network segments. In this scenario, each cluster member with a virtual interface receives all packets. Each gateway decides whether it should take the packet, with one gateway taking responsibility for it. After the initial packet, that gateway is responsible for that connection.



## SecureXL Enhances IPS Performance

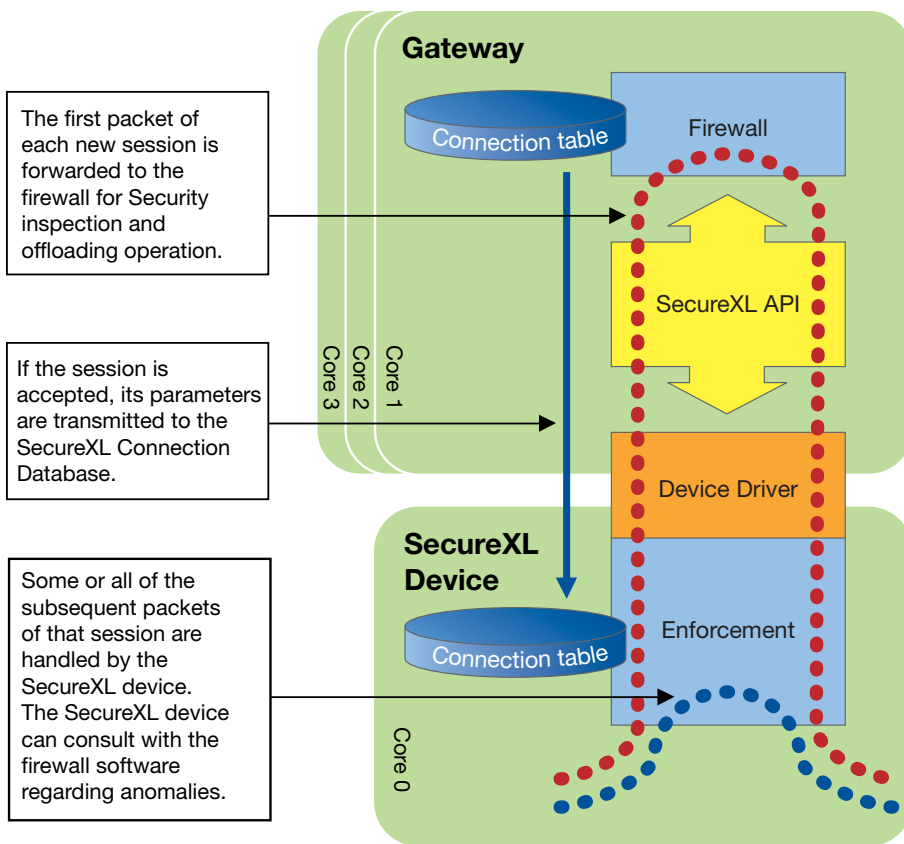
The new TCP streaming engine in Security Gateway R70 uses a new SecureXL API extension to accelerate IPS. The TCP streaming engine puts packets into a data stream so that the IPS parsing engine can extract contexts that match the connection protocol. These contexts are then handed off to the IPS inspection engine which can quickly determine if the content is malicious or not. This brings a new level of performance for integrated IPS.

## SecureXL: Security acceleration

SecureXL is a patented technology consisting of a software package with an API for the acceleration for multiple, intensive security operations. In addition to the IPS, SecureXL also accelerates operations carried out by a Stateful Inspection firewall from Check Point. Through the SecureXL API, this firewall can offload the handling of those operations to a special module, the “SecureXL device,” which is a performance-optimized software module on Power-1 appliances.

In a SecureXL-enabled gateway, the firewall first uses the SecureXL API to query the SecureXL device and discover its capabilities. The firewall then implements a policy that determines which parts of what sessions are to be handled by the firewall, and which should be offloaded to the SecureXL device. When new sessions attempt to get established across the gateway, the first packet of each new session is inspected by the firewall to ensure that the connection is allowed by the security policy. As the packet is inspected, the firewall determines the required behavior for the session, and based on its policy it may then offload some or all of the session handling to the SecureXL device. Thereafter, the appropriate packets belonging to that session are inspected directly by the SecureXL device. The SecureXL device implements the security logic required for further analysis and handling of the traffic. If it identifies anomalies it then consults back with the firewall software and IPS engine. In addition, SecureXL provides a mode that allows for connection setup to be done entirely in the SecureXL device, thus providing extremely high session rate.

### Simplified example of SecureXL process



SecureXL in Multi-core CPU Minimizes Performance Hits to Integrated IPS

Performance is achieved via optimized network interface drivers and multi-threaded code in software. Together, this combination of features increases throughput by a factor of 3X when compared to un-accelerated solutions. The end result is the best price/performance combination on the market. In a multi-core system one or more processors can be assigned to do SecureXL processing and dispatch non-accelerated packets among IPS and firewall kernel instances running on separate cores. SecureXL enables the integrated IPS and firewall to adjust and attain the optimal balance between security and performance requirements.

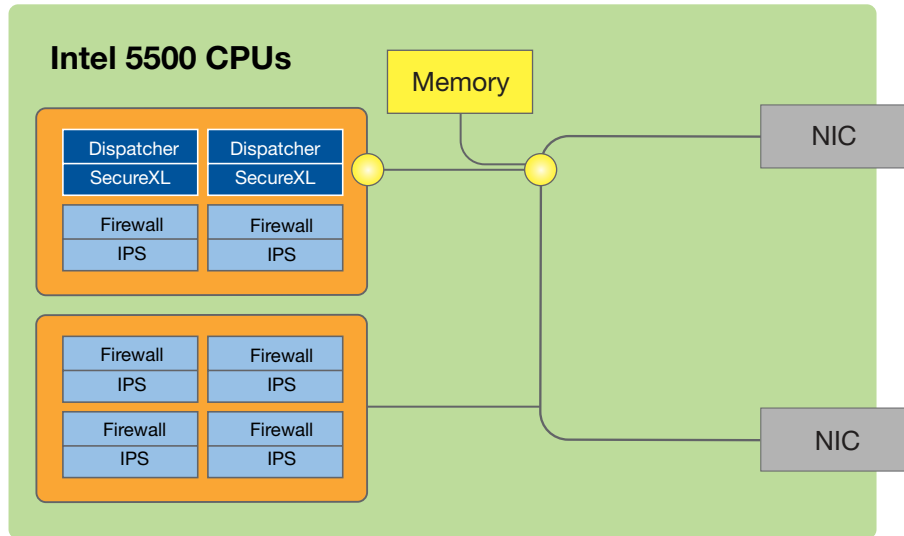
#### CoreXL: Multicore acceleration

CoreXL is the first security technology to fully leverage general-purpose multi-core processors. It introduces advanced load balancing to boost throughput for the deep inspection required to achieve integrated IPS on the firewall. The increased processing capability in multiple cores allows networks to have high performance as well as a high level of security.

#### CoreXL Enhances IPS Performance

IPS engines are distributed among cores in a multi-core system to bring a new level of performance for integrated IPS. In Security Gateway R70 the new IPS engine runs in separate contexts from the firewall instances. As there are multiple firewall instances there are also multiple instances of the IPS engine that run on separate cores. This scales performance by as much as 70% per core.

When CoreXL technology is activated, it immediately assigns one or more cores that are performing SecureXL acceleration to also act as directors for traffic. The other cores are designated to run instances of IPS and firewall on each core. For example, if an appliance contains two quad-core processors, two cores will perform SecureXL acceleration and direct traffic to the other six cores that run IPS and firewall instances. The cores acting as directors have two main functions. First, it makes the initial security decisions whether this traffic can be accelerated by SecureXL. Second, it assigns traffic to a core to handle additional security inspection if needed.



*Multi-core CPUs Enable Dedicated Processing for Integrated IPS*

## Conclusion

The shift from network-layer attacks to dynamically changing application-layer threats has dramatically increased security performance needs. To address them requires an architecture that can quickly evolve to guarantee performance yet maintain a high level of security. While closed, ASIC-based architectures have not been able to make an efficient shift to protecting against application-layer threats. Power-1 provides the foundation needed by large campuses and data centers to gain high performance while maintaining a high level of security.

With three patented technologies integrated within it—ClusterXL, SecureXL, and CoreXL—the performance architecture within Power-1 appliances enables companies to defend against evolving application-layer threats and maintain a predictable level of performance. With this open architecture, organizations can deploy security that delivers on the promise of integrated intrusion prevention without fearing the loss of performance.



## About Check Point Software Technologies Ltd.

Check Point Software Technologies Ltd. ([www.checkpoint.com](http://www.checkpoint.com)), worldwide leader in securing the Internet, is the only vendor to deliver Total Security for networks, data and endpoints, unified under a single management framework. Check Point provides customers uncompromised protection against all types of threats, reduces security complexity and lowers total cost of ownership. Check Point first pioneered the industry with FireWall-1 and its patented stateful inspection technology. Today, Check Point continues to innovate with the development of the Software Blade architecture. The dynamic Software Blade architecture delivers secure, flexible and simple solutions that can be fully customized to meet the exact security needs of any organization or environment. Check Point customers include tens of thousands of businesses and organizations of all sizes including all Fortune 100 companies. Check Point's award-winning ZoneAlarm solutions protect millions of consumers from hackers, spyware and identity theft.

### CHECK POINT OFFICES

#### Worldwide Headquarters

5 Ha'Solelim Street  
Tel Aviv 67897, Israel  
Tel: 972-3-753 4555  
Fax: 972-3-624-1100  
email: [info@checkpoint.com](mailto:info@checkpoint.com)

#### U.S. Headquarters

800 Bridge Parkway  
Redwood City, CA 94065  
Tel: 800-429-4391 ; 650-628-2000  
Fax: 650-654-4233  
URL: <http://www.checkpoint.com>

©2009 Check Point Software Technologies Ltd. All rights reserved. Check Point, AlertAdvisor, Application Intelligence, Check Point Endpoint Security, Check Point Endpoint Security On Demand, Check Point Express, Check Point Express CI, the Check Point logo, ClusterXL, Confidence Indexing, ConnectControl, Connectra, Connectra Accelerator Card, Cooperative Enforcement, Cooperative Security Alliance, CoreXL, CoSa, DefenseNet, Dynamic Shielding Architecture, Eventia, Eventia Analyzer, Eventia Reporter, Eventia Suite, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, FloodGate-1, Full Disk Encryption, Hacker ID, Hybrid Detection Engine, IMsecure, INSPECT, INSPECT XL, Integrity, Integrity Clientless Security, Integrity SecureClient, InterSpect, IPS-1, IQ Engine, MailSafe, NG, NGX, Open Security Extension, OPSEC, OSFirewall, Pointsec, Pointsec Mobile, Pointsec PC, Pointsec Protector, Policy Lifecycle Management, Power-1, Provider-1, PureAdvantage, PURE Security, the puresecurity logo, Safe@Home, Safe@Office, SecureClient, SecureClient Mobile, SecureKnowledge, SecurePlatform, SecurePlatform Pro, SecuRemote, SecureServer, SecureUpdate, SecureXL, SecureXL Turbocard, Security Management Portal, Sentivist, SiteManager-1, Smart-1, SmartCenter, SmartCenter Express, SmartCenter Power, SmartCenter Pro, SmartCenter UTM, SmartConsole, SmartDashboard, SmartDefense, SmartDefense Advisor, Smarter Security, SmartLSM, SmartMap, SmartPortal, SmartProvisioning, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartView Tracker, SMP, SMP On-Demand, SofaWare, SSL Network Extender, Stateful Clustering, Total Security, the totalsecurity logo, TrueVector, Turbocard, UAM, UserAuthority, User-to-Address Mapping, UTM-1, UTM-1 Edge, UTM-1 Edge Industrial, UTM-1 Total Security, VPN-1, VPN-1 Accelerator Card, VPN-1 Edge, VPN-1 Express, VPN-1 Express CI, VPN-1 Power, VPN-1 Power Multi-core, VPN-1 Power VSX, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecuRemote, VPN-1 SecureServer, VPN-1 UTM, VPN-1 UTM Edge, VPN-1 VSX, VSX-1, Web Intelligence, ZoneAlarm, ZoneAlarm Anti-Spyware, ZoneAlarm Antivirus, ZoneAlarm ForceField, ZoneAlarm Internet Security Suite, ZoneAlarm Pro, ZoneAlarm Secure Wireless Router, Zone Labs, and the Zone Labs logo are trademarks or registered trademarks of Check Point Software Technologies Ltd. or its affiliates. ZoneAlarm is a Check Point Software Technologies, Inc. Company. All other product names mentioned herein are trademarks or registered trademarks of their respective owners. The products described in this document are protected by U.S. Patent No. 5,606,668, 5,835,726, 5,987,611, 6,496,935, 6,873,988, 6,850,943, and 7,165,076 and may be protected by other U.S. Patents, foreign patents, or pending applications.